Unit 12A Depot Plaza
13-25 Main Street
Franklin, MA 02038
(800) 360-4010

April 1, 2003

Mary Cottrell, Secretary
Department of Telecommunications and Energy
One South Station, 2nd Floor
Boston, MA 02110

RE: D.T.E. 03-38 – Request for Comments

CC: List of registered Competitive Local Exchange Carriers in Massachusetts

In comment on Verizon's petition for waiver of certain service results, citing a "worm" as the reason for their intentional closure and denial of service, shutting down its wholesale interfaces, during the weekend of January 25, 2003, NCI telecom would like to offer the following words for consideration:

In this case, it appears that Verizon chose to shut down its service or block access entirely to that service to protect itself from such an attack. The problem is that so many businesses depend on access to the Verizon Wholesale Interfaces that such an act causes damages and losses to those businesses affected. Orders for new service can not get processed in time and then prospective customers may choose to leave, taking their business directly to Verizon themselves or proceeding to other carriers. Orders for cancellation or changes can not get processed and may cause additional cost to the customer, losses in potential business or opportunity cost. A company like Verizon that has contracted with resellers and requires them to use this electronic interface must understand the potential damage it can cause by making such a decision to close its access, without adequate notice or alternative systems in place before doing so.

Verizon, with its large size and resources should have been able to protect itself to a better degree and not arbitrarily decide to stop service based on a perceived threat rather than an actual system failure or breach. Frequent backups of database information, redundant servers and network systems, firewalls, specialized software, and other preventative measures should be in place to protect Verizon systems from attack. In the event of such a "worm" virus, Verizon should be able to provide redundant interfaces, from separate locations or networks that would not be affected or infected. There are new "worms" coming out every day. What is Verizon's "Performance Assurance Plan"? One would expect Verizon to at least offer a second means to provide wholesalers access or be able to process wholesale orders in case of such an outage or disruption. Examples might be to accept fax transmittals to CLEC account managers, or to have a regional, 24x7 emergency department that could internally process the orders until the electronic system was again available, or to expect to pay credits and liquidated damages and have an insurance plan to cover those claims.

The Internet, as known to most people who use it, is largely insecure, an electronic environment which can leave anyone connected to it at risk from, "hackers", "viruses", "spam email" and "worms". It should go without saying that any businesses that wish to provide electronic commerce and/or access to their internal networks and databases must protect themselves from such risks or potential attacks using whatever means available, within their

financial constraints. If they can not afford to protect themselves, then they should expect that at some time they might face the inevitable service or network attack that may or may not cause system downtime, damage or loss.

Please consider that the amounts requested by the resellers and/or CLECs to credit them for the system outage, directly controlled by Verizon, is only $164,000. This total amount seems very small compared to the potential business loss and opportunity cost that was endured by each of the claimants or any party that depends on the Verizon Wholesale Interfaces. It should be expected that a much larger amount of loss, perhaps in the millions for all the CLECs, resellers, and hundreds of thousands of customers affected, may have been realized.

Verizon should not be waived in crediting those requesting parties for the service denial on account of this "worm". They should be held accountable for their actions or inaction. Otherwise, what is to stop Verizon from claiming the "worm" for any type of network related outage or denial of service. It would certainly be arguable on their part that every system may be networked to some other type of computer or machine, telephone switch, or other component on their network that perhaps could be directly or indirectly connected to the Internet and may therefore be at risk of attack. At what point does the public and their representatives hold Verizon accountable for its business practices. You don't see, for example, a power company shutting off the power just for any "worm" threat, when the computers that control the power grids and systems may be indirectly connected to the Internet and could conceivably be at risk.

NCI telecom recommends the Department of Telecommunications and Energy deny Verizon's petition for waiver of certain service results on the grounds that those results were caused by Verizon's willfull denial of service rather than proven actual system failure from a "worm" virus attack. Verizon system shut down should not be one of the precautions taken to avoid Internet related attacks, it should be a last resort or direct result of attack and there should be Verizon backup systems or alternatives already in place to handle such an event. Verizon should be further directed and held liable to pay those credits filed in full within 30 days or less or risk further action and/or liability. Nothing in any order should affect any direct legal action that the credit requesting parties may attempt in order to recoup other related damages or losses that may not have been filed.

Thank you for the opportunity to submit these comments in regards to this matter and we hope the Department of Telecommunication and Energy considers the opinion of NCI telecom.

Sincerely,

Nathaniel S. Morse
President
NCI telecom